CLAIMS

1-50. (cancelled)

51. (previously presented) A method of thwarting detection of a secret binary number in a cryptographic computational device by analysis of externally observable parameters, comprising:

conditionally performing a plurality of calculations in response to the bit values of said secret number;

multiplicatively accumulating the results of said plurality of calculations in a subtotal; and

performing dummy calculations in response to selected bit positions of said secret number that indicate calculations should not be performed, and not multiplicatively accumulating the results of the dummy calculations in said subtotal, said selected bit positions randomly distributed over a binary indicator equal in length to said secret number;

whereby said dummy calculations alter at least one externally observable parameter.

52. (previously presented) The method of claim 51 wherein conditionally performing a plurality of calculations in response to the bit values of said secret number comprises performing a calculation where said bit value is a one and not performing said calculation where said bit value is a zero.

53. (previously presented) The method of claim 52 wherein performing dummy calculations in response to selected bit positions of said secret number that indicate calculations should not be performed comprises performing said dummy calculations in response to said secret number bit position being a zero and a corresponding indicator bit position being a one.

54-55. (cancelled)

56. (previously presented) The method of claim 53 wherein said indicator is fixed.

57. (previously presented) The method of claim 56 wherein said indicator is generated upon first commissioning said device into operation and internally stored such that it is never released outside said device.

58. (previously presented) The method of claim 51 further comprising generating said secret number upon first commissioning said device into operation and internally storing said secret number such that it is never released outside said device.

59. (previously presented) The method of claim 51 in which said externally observable parameters include variation in power supply current.

60. (previously presented) The method of claim 51 in which said externally observable parameters include variation in timing of outputting results of said calculations.

61. (previously presented) The method of claim 51 wherein conditionally performing a plurality of calculations and accumulating their results calculates the exponentiation of a long integer to the power of a large secret exponent.

62. (previously presented) The method of claim 61 in which calculating the exponentiation of a long integer to the power of a large secret exponent comprises selectively calculating successive squares of said long integer and multiplicatively accumulating said squares in

response to the bit values of said secret exponent, and reducing said accumulated value modulo a given modulus.

63-72. (cancelled)

73. (previously presented) A detection-proof computational device comprising:

an input/output interface;

a memory storing a secret binary number; and

a processor operatively connected to said input/output interface and to said memory and programmed for cryptographic computation using said secret binary number while thwarting detection of said secret binary number by analysis of externally observable parameters, the cryptographic computation comprising:

conditionally performing a plurality of calculations in response to the bit values of said secret number;

multiplicatively accumulating the results of said plurality of calculations in a subtotal; and

performing dummy calculations in response to selected bit positions of said secret number that indicate calculations should not be performed, and not multiplicatively accumulating the results of the dummy calculations in said subtotal, said selected bit positions randomly distributed over a binary indicator equal in length to said secret number;

whereby said dummy calculations alter at least one externally observable parameter.

74-75. (cancelled)

76. (previously presented) The device of claim 73 in which in which said externally observable parameters include variation in power supply current.

77. (previously presented) The device of claim 73 in which said externally observable parameters include variation in timing of outputting results of said calculations.

78. (previously presented) The device of claim 73 wherein said secret cryptographic computations comprise exponentiating a long integer to the power of a large secret exponent.

79. (previously presented) The device of claim 78 wherein exponentiating a long integer to the power of a large secret exponent comprises selectively calculating successive squares of said long integer and multiplicatively accumulating said squares in response to the bit values of said secret exponent, and reducing said accumulated value modulo a given modulus.

80 – 87. (cancelled)

88. (previously presented) A mobile terminal used in a mobile communications system comprising:

a transmitter and a receiver for communicating in the mobile communications system;

a controller controlling operation of the transmitter and the receiver; and

a secure device removably, operatively connectable to the controller and comprising:

an input/output interface;

a memory storing a secret binary number; and

a processor operatively connected to said input/output interface and to said memory and programmed for cryptographic computation using said secret binary number while thwarting detection of said secret binary number by analysis of externally observable parameters, the cryptographic computation comprising:

conditionally performing a plurality of calculations in response to the bit values of said secret number;

multiplicatively accumulating the results of said plurality of calculations in a subtotal; and

performing dummy calculations in response to selected bit positions of said secret number that indicate calculations should not be performed, and not multiplicatively accumulating the results of the dummy calculations in said subtotal, said selected bit positions randomly distributed over a binary indicator equal in length to said secret number;

whereby said dummy calculations alter at least one externally observable parameter.

89-90. (cancelled)

91. (previously presented) The mobile terminal of claim 88 in which in which said externally observable parameters include variation in power supply current.

92. (previously presented) The mobile terminal of claim 88 in which said externally observable parameters include variation in timing of outputting results of said calculations.

93. (previously presented) The mobile terminal of claim 88 wherein said secret cryptographic computations comprise exponentiating a long integer to the power of a large secret exponent.

94. (previously presented) The mobile terminal of claim 93 wherein exponentiating a long integer to the power of a large secret exponent comprises selectively calculating successive squares of said long integer and multiplicatively accumulating said squares in response to the bit values of said secret exponent, and reducing said accumulated value modulo a given modulus.

95 – 106. (cancelled)